PCT/JP99/02510

EJ

17.06.99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

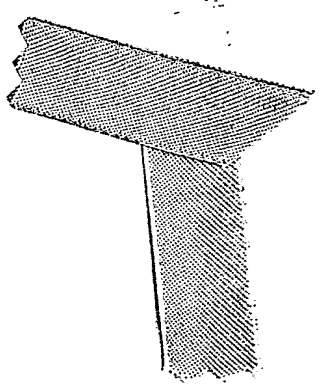
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ５月１８日

出 願 番 号
Application Number: 平成１０年特許願第１３５５０２号

出 願 人
Applicant (s): 三菱マテリアル株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



１９９９年 ４月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０２１０７９

【書類名】　特許願

【整理番号】　SOMC0212A

【提出日】　平成10年 5月18日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

G06F 12/00

H04L 9/00

【発明の名称】　情報共有システム、情報保管装置およびそれらの情報処理方法、並びに記録媒体

【請求項の数】　20

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社総合研究所内

【氏名】　大久保　達真

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社総合研究所内

【氏名】　豊田　祥一

【特許出願人】

【識別番号】　000006264

【氏名又は名称】　三菱マテリアル株式会社

【代表者】　秋元　勇巳

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9802373

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報共有システム、情報保管装置およびそれらの情報処理方法、並びに記録媒体

【特許請求の範囲】

【請求項１】　共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、

少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、

情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化手段と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送手段と、上記情報保管装置からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送するリスト管理手段と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化手段とを有する暗号化復号化装置とを備えた情報共有システム。

【請求項２】　上記暗号化復号化装置は、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得し、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成し、上記転送手段に出力する手段を

さらに有する請求項１記載の情報共有システム。

【請求項３】　共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくと

もグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーを追加登録または削除する場合、上記情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、

作成したグループリストを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項４】　共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーで利用する共通鍵を登録する場合、上記情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

暗号化された共通鍵を上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項５】　共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管

されている情報共有システムの情報処理方法であって、

上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項６】　共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

を有する情報共有システムの情報処理方法。

【請求項７】　少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、

作成したグループリストを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項８】　少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

暗号化された共通鍵を上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項９】　少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１１】　少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置であって、

グループリスト変更要求に応答して上記グループリストを変更可能なグループリスト管理手段と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録し、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する共通鍵管理手段と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管し、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する暗号化データ管理手段とを有する情報保管装置。

【請求項１２】　上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する

請求項１１記載の情報保管装置。

【請求項１３】　上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する

請求項１１または１２記載の情報保管装置。

【請求項１４】　少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置の情報処理方法であって、

グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

を有する情報保管装置の情報処理方法。

【請求項１５】　特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程

をさらに有する請求項１４記載の情報保管装置の情報処理方法。

【請求項１６】　特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程

をさらに有する請求項１４または１５記載の情報保管装置の情報処理方法。

【請求項１７】　グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能

な記録媒体。

【請求項１８】　グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１９】　グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２０】　グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数のユーザ間での情報共有を目的とし、情報の覗き見や改竄を防ぐための情報共有システムおよびその情報処理方法、並びに記録媒体に関するものである。

【０００２】

【従来の技術】

近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報が

コンピュータネットワーク上で利用されるようになった。

しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。

そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

【０００３】

このような秘匿する必要のある情報を暗号化するために、データ暗号規格（ＤＥＳ；Data Encryption Standard）などの共通鍵暗号方式が開発された。

この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要があった。

そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する手段が提案されている。

【０００４】

ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理する鍵管理システムや、情報を共有するユーザをグループ化して管理するグループ管理サーバ、情報へのアクセス制御手段などを利用する必要がある。

【０００５】

【発明が解決しようとする課題】

このように特定グループで秘匿データを共有する場合の共通鍵管理は、サーバで行われ、このサーバにはサーバ管理者が設けられる。

ところが、このサーバ管理者が当該特定グループに含まれない場合には、何の障害もなくデータを覗くことができることになる。

また、サーバ管理者が当該特定グループに含まれたとしても、一存でグループメンバーを変更することができ、データの管理上、万全であるとはいえない。

【０００６】

本発明は、かかる事情に鑑みてなされたものであり、その目的は、暗号化情報

を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改ざんを防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】

上記目的を達成するため、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化手段と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送手段と、上記情報保管装置からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送するリスト管理手段と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化手段とを有する暗号化復号化装置とを備えている。

【０００８】

また、本発明の情報共有システムでは、上記暗号化復号化装置は、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得し、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成し、上記転送手段に出力する手段を、さらに有する。

【０００９】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、グループに属するメンバーを追加登録または削除する場合、上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、作成したグループリストを上記情報保管装置に転送する工程とを有する。

【００１０】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、グループに属するメンバーで利用する共通鍵を登録する場合、上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、暗号化された共通鍵を上記情報保管装置に転送する工程とを有する。

【００１１】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、この暗号化鍵情報から

共通鍵を復号する工程と、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、暗号化されたデータを上記情報保管装置に転送する工程とを有する。

【００１２】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で取得した暗号化データを復号する工程とを有する。

【００１３】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、作成したグループリストを上記情報保管装置に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【００１４】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、暗号化された共通鍵を上記情報保管装置に転送する工程とをコンピュータに実

行させるプログラムが記録されている。

【００１５】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、暗号化されたデータを上記情報保管装置に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【００１６】

また、本発明の記録媒体は、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で取得した暗号化データを復号する工程とをコンピュータに実行させるプログラムが記録されている。

【００１７】

また、本発明は、少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置であって、グループリスト変更要求に応答して上記グループリストを変更可能なグループリスト管理手段と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録し、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する共通鍵管理手段と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管し、暗号化データの取得データに応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送す

る暗号化データ管理手段とを有する。

【００１８】

また、本発明では、上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する。

【００１９】

また、本発明では、上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する。

【００２０】

また、本発明は、少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置の情報処理方法であって、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程とを有する。

【００２１】

また、本発明では、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程をさらに有する。

【００２２】

また、本発明では、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程をさらに有する。

【００２３】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【００２４】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【００２５】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先

に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【００２６】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【００２７】

本発明によれば、複数ユーザが共有したい情報を秘匿しておくために、たとえば共有鍵暗号方式と公開鍵暗号方式が併用される。入力情報は、共有鍵暗号方式で、共通鍵を用いて暗号化される。

【００２８】

また、本発明によれば、たとえばネットワーク上での情報共有システムが実現される。

このシステムでは、少なくとも複数のメンバーでアクセス可能な情報保管装置

に、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管される。

【００２９】

グループに属するメンバーを追加登録する場合、情報保管装置からグループリストが取得され、取得したグループリストのグループ管理者の署名が指定された署名と一致するか否かを判断される。

そして、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストが作成され、作成されたグループリストが情報保管装置に転送され保管される。

【００３０】

また、グループに属するメンバーで利用する共通鍵を登録する場合、情報保管装置からグループリストが取得され、取得したグループリストのグループ管理者の署名が指定された署名と一致するか否かを判断される。

そして、一致する場合にのみ、指定されている公開鍵を用いて登録すべき共通鍵が暗号化され、暗号化された共通鍵が情報保管装置に転送され保管される。

【００３１】

また、共通鍵を用いてデータを暗号化する場合、情報保管装置の共通鍵リストから少なくとも暗号化鍵情報が取得され、この暗号化鍵情報から共通鍵が復号される。

そして、復号した共通鍵で共通鍵暗号化方式に基づいて入力情報が暗号化されて暗号化データが生成され、暗号化されたデータが情報保管装置に転送され保管される。

【００３２】

また、データを復号する場合には、情報保管装置から所望の暗号化鍵情報および暗号化データが取得され、この暗号化鍵情報から共通鍵が復号されり。

そして、復号した共通鍵で取得した暗号化データが復号される。

【００３３】

また、情報保管装置では、グループリスト変更要求があると、グループ管理手段により要求に応じたグループリストの変更が行われる。

また、共通鍵の登録要求があると、共通鍵管理手段により、要求のあった共通鍵がその暗号化鍵情報を含めて登録される。また、共通鍵の取得要求があると、共通鍵管理手段により、特定グループでの情報共有に最適な共通鍵が選択されて、要求先に転送される。

また、暗号化データの登録要求があると、暗号化データ管理手段により、暗号化データが当該データの暗号化に用いられた共通鍵情報とともに保管される。また、暗号化データの取得要求があると、暗号化データ管理手段により、保管暗号化データおよび共通鍵情報が要求先に転送される。

【００３４】

【発明の実施の形態】

以下、本発明の実施形態を図面に関連付けて詳細に説明する。

【００３５】

図１は本発明に係る情報共有システムの基本的な構成図、図２は本発明に係る暗号化復号化装置の構成例を示すブロック図である。

【００３６】

本実施形態に係る情報共有システムは、図１に示すように、図２に示す暗号化復号化装置１０が組み込まれた第１の端末装置１および第２の端末装置２、並びに暗号化復号化装置１０で生成されたグループリストや、共通鍵リスト、暗号化データ等を保管するための情報保管装置としてのＷＷＷサーバ３が、ネットワーク（たとえば、インターネット）４で接続されて構成されている。

【００３７】

暗号化復号化装置１０は、暗号化部１１、共通鍵生成部１２、記憶部１３、暗号化鍵生成部１４、付加情報生成部１５、転送部１６、署名確認部１７、公開鍵管理部１８、署名付加部１９、並びに復号化部２０により構成されている。

そして、署名確認部１７、公開鍵管理部１８、および署名付加部１９を主要素としてリスト管理手段が構成される。

【００３８】

暗号化部１１は、情報を暗号化するための共通鍵ｄｋまたはＷＷＷサーバ３から読み出した共通鍵ｃｋを用いて、たとえば共有鍵暗号方式（たとえばＤＥＳ）

により入力情報Ｍを暗号化して暗号化データＭ’を生成し、生成した暗号化データＭ’を転送部１６に出力する。

また、暗号化部１１は、グループで共通鍵を共有する場合であって、データを暗号化する場合に、特定グループのグループリスト要求、具体的にはグループＩＤやユーザ公開鍵ＩＤを含むグループリスト要求をＷＷＷサーバ３に対して行う。この要求の転送は転送部１６を介して行われる。

【００３９】

共通鍵生成部１２は、たとえば乱数発生回路等により構成され、情報を暗号化するための共通鍵ｄｋを生成し、暗号化部１１および暗号化鍵生成部１４に出力する。なお、共通鍵ｄｋは、たとえば６４ビットデータとして生成される。

【００４０】

記憶部１３は、たとえばハードディスクにより構成され、本システムを共有する複数ｎのユーザ各々の固有の公開鍵ＰＫ１，ＰＫ２，…，ＰＫｎがあらかじめ記録されており、暗号化鍵生成部１４および公開鍵管理部１８によりアクセスされる。

【００４１】

暗号化鍵生成部１４は、暗号化に用いた共通鍵ｄｋ（または共通鍵ｃｋ）を、記憶部１３に記録されているユーザの公開鍵を用い、たとえば公開鍵暗号方式（たとえばＲＳＡ）に基づいて暗号化し、１または複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎを生成し、生成した暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎを転送部１６に出力する。

また、暗号化鍵生成部１４は、特定グループに属するメンバーだけで情報を共有したい場合であって、そのメンバーで利用する共通鍵の登録を行う場合、特定グループのグループリスト要求をＷＷＷサーバ３に対して行う。この要求の転送は転送部１６を介して行われる。

【００４２】

付加情報生成部１５は、たとえば共通鍵ｄｋのメッセージダイジェストｋｍｄをハッシュ関数などで生成し、付加情報ａｊｆとして転送部１６に出力する。

なお、付加情報としては、ユーザの秘密鍵で復号化できる暗号化鍵を特定する

ための、ＩＤ、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報であってもよい。

【００４３】

転送部１６は、入力情報Ｍの暗号化に伴って生成された１または複数の暗号化鍵ＥＫ１，ＥＫ２，…，ＥＫｎ、暗号化データＭ’、および付加情報ａｊｆをネットワーク４を介して情報保管装置としてのＷＷＷサーバ３に転送する。

なお、共通鍵の登録時には転送処理を行わない。

【００４４】

署名確認部１７は、ＷＷＷサーバ３に保管されている特定グループに属する公開鍵のグループリストＧＬをネットワーク４を介して受けて、グループ管理者のデジタル署名（Ｄ署名）を確認し、確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、その公開鍵ＰＫを記憶部１３から公開鍵管理部１８に出力させ、脱会するメンバーがあるときには受け取ったグループリストに記載されているメンバーから該当メンバーを削除させ、また、共有鍵を登録するときには、公開鍵ＩＤリストに応じた公開鍵ＰＫを記憶部１３から暗号化鍵生成部１４に出力させる。

【００４５】

公開鍵管理部１８は、新規にグループに加入するユーザの公開鍵を追加するときに、記憶部１３から出力された指定公開鍵ＰＫを受けて、新しいグループリストを作成し、公開鍵番号（Ｎｏ）、メンバーの公開鍵をリストに設定し、さらに新規のグループリストに対してグループＩＤを付加して署名付加部１９に出力する。また、たとえば特定グループのグループリスト要求等が発生した場合、この要求をＷＷＷサーバ３に対して行う。

【００４６】

署名付加部１９は、公開鍵管理部１８による新規のグループリストに対してグループ管理者のデジタル署名を付加し、ネットワーク４を介して情報保管装置としてのＷＷＷサーバ３に転送し、登録させる。

【００４７】

復号化部２０は、特定グループで共通鍵を共有している場合には、ＷＷＷサー

バ３に登録されている共通鍵リストＣＫＬの中から所望の共通鍵番号（Ｎｏ）、暗号化鍵を取得し、公開鍵暗号方式（たとえば、ＲＳＡ）を用いてユーザの秘密鍵ｐｖｋで暗号化鍵を復号して共通鍵を取得し、暗号化部１１に出力する。

また、WWWサーバ３に登録されているデータを復号する場合には、データＩＤ，公開鍵番号（Ｎｏ）をWWWサーバ３に転送して、暗号化鍵およびデータを取得し、公開鍵暗号方式を用いて、共通鍵を復号し、共通鍵暗号方式を用いてデータを復号する。

この復号部２０は、図３に示すように、暗号化鍵復号化部２１、情報復号化部２２により構成される。

【００４８】

なお、復号化部２０は、たとえばWWWサーバ３に複数の暗号化鍵、付加情報、および暗号化データに加えて保管されている共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報ｄｅｓｒｓａ（たとえば、ＤＥＳとＲＳＡで暗号化した、など）や、暗号化アルゴリズムの実行に必要な上記以外の情報ｉｎｆｏ（たとえば、ＤＥＳに利用した初期化乱数など）も、取得する。

そして、たとえば、アルゴリズム識別情報ｄｅｓｒｓａ、情報ｉｎｆｏに基づいて、復号化に利用できるように、アルゴリズムを初期化する処理等も行う。

【００４９】

WWWサーバ３は、図４に示すように、データベースマネージメントシステム（ＤＢＭＳ）３１および権限確認機能を有する権限確認部３２を有しており、グループリストＧＬ、共通鍵リストＣＫＬ、グループの共通鍵リストＧＣＫＬ、暗号化データリストＥＤＬ、およびデータ共通鍵リストＤＣＫＬを所定の記憶部に記録し、保管する。

【００５０】

ＤＢＭＳ３１は、図５に示すように、グループリスト管理部３１１、共通鍵管理部３１２、および暗号化データ管理部３１３の３つの情報管理保管機能を有している。これらの機能は、権限確認機能を利用して、各変更や登録、データ保管要求が権限を満たしているか否かを確認する。

【００５１】

グループリスト管理部３１１は、クライアント側からのグループリスト変更要求時に、グループリストＧＬにアクセスして、メンバー変更要求に対して応答し、返信されてきたグループ管理者の要求に従ってグループリストＧＬを変更する。また、グループリスト管理部３１１は、グループ全体を追加・削除する機能を有している。

【００５２】

共通鍵管理部３１２は、共通鍵登録時に、共通鍵リストＣＫＬとグループの共通鍵リストＧＣＫＬにアクセスし、共通鍵の登録を行う。

共通鍵管理部３１２は、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵（特定グループで複数の共通鍵（随時更新されていく）を有している場合には、最新の共通鍵）を選択して、クライアントに転送する。また、たとえば登録対象の共通鍵に関する暗号化鍵、グループＩＤ情報を受信したならば、各リストに振り分けて保管する。そのとき、共通鍵ＩＤを生成する。

【００５３】

また、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合には、グループリスト管理部３１１および共通鍵管理部３１２は協働して以下に示すような処理を行う。

【００５４】

この場合、グループリスト管理部３１１は、権限を確認するとともに、グループＩＤを参照して特定グループに属するメンバーの公開鍵番号（Ｎｏ）、公開鍵をグループリストＧＬより取得する。

共通鍵管理部３１２は、グループの共通鍵リストＧＣＫＬよりグループＩＤを参照して、特定グループで利用されている共通鍵番号（Ｎｏ）を全て検索する。そして、共通鍵リストＣＫＬより、各共通鍵番号（Ｎｏ）とグループ管理者の公開鍵番号（Ｎｏ）が一致する全ての暗号化鍵を取得し、クライアントに転送する。

そして、グループリスト管理部３１１および共通鍵管理部３１２は、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とグループリスト、公開鍵番号（Ｎｏ）と共通鍵ＩＤを受けて、グループリストＧＬ、共通鍵リストＣＫＬ、グループの共通鍵リストＧＣＫＬを変更する。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含まれているので、過去の共有情報を、取得することができる。

【００５５】

また、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合、グループリスト管理部３１１および共通鍵管理部３１２は、協働して以下に示すような処理を行う。

【００５６】

この場合、グループリスト管理部３１１は、グループリストの更新を行う。最後の返信部分では、新しいグループリストと更新前のグループリストとを比較し、削除したメンバーの公開鍵番号（Ｎｏ）を割り出し、グループＩＤと削除したメンバーの公開鍵番号（Ｎｏ）を共通鍵管理部３１２にわたす。

共通鍵管理部３１２は、グループの共通鍵リストＧＣＫＬより、グループＩＤを参照して、特定グループで利用されていた共通鍵番号（Ｎｏ）を全て検索し、共通鍵リストＣＫＬより、各共通鍵番号（Ｎｏ）と削除したメンバーの公開鍵番号（Ｎｏ）が一致する全ての暗号化鍵を削除する。

【００５７】

なお、ＤＢＭＳ３１では、メンバーの追加と削除が同時に行われた場合には、上述した手法が組み合わされて実行される。

【００５８】

暗号化データ保管部３１３は、共通鍵管理部３１２と協働して、グループの共通鍵リストＧＣＫＬ、共通鍵リストＣＫＬ、データ共通鍵リストＤＣＫＬ、暗号化データリストＥＤＬをアクセスし、クライアントの要求に従ってグループリストの送信と暗号化データの受付を行い、データＩＤを生成する。また、復号化要求を受け取った場合には、データＩＤと公開鍵番号（Ｎｏ）を参照し、３つのリ

ストを参照して暗号化データと暗号化鍵を返信する。

【００５９】

次に、上記構成による動作を説明する。

なお、ここでは、グループで共通鍵を共有する場合であって、グループへの公開鍵ＩＤの登録例、共通鍵の登録例、データの暗号化および登録例、共通したいユーザを別途指定する場合の暗号化例、並びにデータの復号化例について、図６～図１０に関連付けて順を追って説明する。

【００６０】

まず、グループで共通鍵を共有する場合であって、グループへの公開鍵ＩＤの登録例について図６に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、まず、グループに属するメンバーの公開鍵ＩＤの登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのグループリスト要求がWWWサーバ３に対して、たとえば公開鍵管理部１８から行われる（Ｓ６１）。

【００６１】

グループリスト要求に対して、WWWサーバ３から特定グループに属する公開鍵ＩＤリストがネットワーク４を介してクライアント側暗号化復号化装置１０に転送される（Ｓ６２）。

暗号化復号化装置１０では、署名確認部１７にこの公開鍵リストであるグループリストが入力され、ここでグループ管理者のデジタル署名の確認が行われる（Ｓ６３）。

確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、その公開鍵ＰＫが記憶部１３から公開鍵管理部１８に出力され、脱会するメンバーがあるときには受け取ったグループリストに記載されているメンバーから該当メンバーの公開鍵が削除される（Ｓ６４）。

【００６２】

公開鍵管理部１８では、記憶部１３から出力された指定公開鍵ＰＫを受けて、新しいグループリストが作成され（Ｓ６５）、公開鍵番号（Ｎｏ）、メンバーの

公開鍵、およびグループＩＤがリストに設定されて、署名付加部１９に出力される。

【００６３】

署名付加部１９において、公開鍵管理部１８による新規のグループリストに対してグループ管理者のデジタル署名が付加される（Ｓ６６）。

そして、たとえば署名付加部１９からグループリスト更新要求がWWWサーバ３に対して行われ、WWWサーバ３においてグループリスト管理部３１１によりグループリストＧＬの更新が行われる（Ｓ６７）。

【００６４】

なお、ステップＳ６３において、署名確認が否定的である場合には、当該グループ管理者はグループリスト等の更新、削除等を行う権限のないものとして、ステップＳ６４以降の処理は行われない。

【００６５】

次に、グループで共通鍵を共有する場合であって、共通鍵の登録例について図７に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、そのメンバーで利用する共通鍵の登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのグループリスト要求がWWWサーバ３に対して、たとえば暗号化鍵生成部１４から行われる（Ｓ７１）。

【００６６】

グループリスト要求に対して、WWWサーバ３から特定グループに属する公開鍵ＩＤリストがネットワーク４を介してクライアント側暗号化復号化装置１０に転送される（Ｓ７２）。

暗号化復号化装置１０では、署名確認部１７にこの公開鍵リストであるグループリストが入力され、ここでグループ管理者のデジタル署名の確認が行われる（Ｓ７３）。

【００６７】

確認が肯定的である場合、公開鍵ＩＤリストに応じた公開鍵ＰＫが記憶部１３

から暗号化鍵生成部１４に出力される。

暗号化鍵生成部１４では、共通鍵生成部１２で生成された共通鍵Ｓｋｅｙ１が、与えられた公開鍵を用いてたとえば公開鍵暗号方式に基づいて暗号化され、図７に示すように、公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データを付加して１または複数の暗号化鍵ＥＫが生成され、転送部１６に出力される（Ｓ７４）。

そして、転送部１６により公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データが付加された暗号化鍵を含む共通鍵リストデータがネットワーク４を介してＷＷＷサーバ３に転送され、共通鍵管理部３１２により図７に示すように所定の場所に保管される（Ｓ７５）。

なお、転送場１６から転送される情報には、付加情報生成部１５で生成された付加情報が含まれる場合もある。

【００６８】

なお、ステップＳ７３において、署名確認が否定的である場合には、当該グループ管理者は共通鍵の登録を行う権限のないものとして、ステップＳ７４以降の処理は行われない。

【００６９】

次に、グループで共通鍵を共有する場合であって、データを暗号化する場合について図８に関連付けて説明する。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのグループリスト要求、具体的にはグループＩＤ、ユーザ公開鍵ＩＤ（たとえば番号「ＩＣ：ＦＦ」）の要求がＷＷＷサーバ３に対して、たとえば暗号化部１１から行われる（Ｓ８１）。

【００７０】

グループリスト要求に対して、ＷＷＷサーバ３から特定グループに属する共通鍵（たとえば「１２２」）、暗号化鍵（「ｚｘｃｖ」）がネットワーク４を介してクライアント側暗号化復号化装置１０に転送される（Ｓ８２）。

【００７１】

暗号化復号化装置１０では、復号化部２０において、共通鍵番号（１２２）、

暗号化鍵（ｚｘｃｖ）が取得され、公開鍵暗号方式を用いてユーザの秘密鍵ｐｖｋで暗号化鍵が復号されて共通鍵Ｓｋｅｙ２が取得され、暗号化部１１に出力されれる（Ｓ８３，Ｓ８４）。

【００７２】

暗号化部１１では、入力情報Ｍ（「こんにちは」）が入力され、この入力情報Ｍが共有鍵暗号方式（たとえば、ＤＥＳ）に基づいて共通鍵Ｓｋｅｙ２を用いて暗号化され、共通鍵番号（１２２）が付加された暗号化データＭ’（たとえば「jjjjjjjjjjjjj」）が生成されて転送部１６に出力される（Ｓ８５）。

そして、転送部１６により共通鍵番号（１２２）が付加された暗号化データＭ’（たとえば「jjjjjjjjjjjjj」）がネットワーク４を介してＷＷＷサーバ３に転送され、暗号化データ管理部３１３により図８に示すように所定の場所に保管される（Ｓ８６）。

【００７３】

次に、共有したいユーザを別途指定する場合であって、データを暗号化する場合について図９に関連付けて説明する。

この場合、入力情報Ｍ（「こんにちは」）が暗号化装置１０の暗号化部１１に入力される。このとき、共通鍵生成部１２で、共通鍵Ｓｋｅｙ１が生成され（Ｓ９１）、この共通鍵Ｓｋｅｙ１が暗号化部１２および暗号化鍵生成部１４に供給される（Ｓ９２，Ｓ９３）。

【００７４】

暗号化部１１では、入力情報Ｍが共有鍵暗号方式ＤＥＳに基づいて共通鍵Ｓｋｅｙ１を用いて暗号化され、共通鍵番号（たとえば「１２４」）が付加された暗号化データＭ’（たとえば「jjjjjjjjjjjjj」）が生成されて転送部１６に出力される。

【００７５】

また、暗号化鍵生成部１４によって、ユーザＡ、Ｂ、Ｃの公開鍵暗号方式（たとえば、ＲＳＡ）に基づいた公開鍵ＰＫが記憶部１３から読み出される。

暗号化鍵生成部１４において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて共通鍵Ｓｋｅｙ１が暗号化され、たとえば暗号化鍵（ｏｌｋｊ

，Ｏｉｗｉ，Ｘｋｎｍ）が得られ、公開鍵番号（「１１：ＡＡ」、「１Ｃ：ＦＦ」、「Ｅ５：４Ｂ」）を含むデータが転送部１６に出力される（Ｓ９４）。

そして、転送部１６により共通鍵番号（たとえば「１２４」）が付加された暗号化データＭ’（たとえば「ｊｊｊｊｊｊｊｊｊｊｊｊｊ」）、並びに暗号化鍵（ｏｌｋｊ，Ｏｉｗｉ，Ｘｋｎｍ）、公開鍵番号（「１１：ＡＡ」、「１Ｃ：ＦＦ」、「Ｅ５：４Ｂ」）を含むデータがネットワーク４を介してＷＷＷサーバ３に転送され、図９に示すように所定の場所に保管される（Ｓ９５）。

【００７６】

次に、ＷＷＷサーバ３に保管されているデータを取得する場合を、図１０に関連付けて説明する。

この場合、たとえば復号化部２０からデータＩＤ（たとえば「４４４４」）、公開鍵ＩＤが、ＷＷＷサーバ３に対して送信される（Ｓ１０１）。

ＷＷＷサーバ３では、受けたデータＩＤおよびこれに基づく共通鍵番号（たとえば「１２２」）により、暗号化データ（たとえば「ｊｊｊｊｊｊｊｊｊｊｊｊｊ」）およびこれに対応した暗号化鍵（ｚｘｃｖ）が暗号化データ管理部３１３により所定の保管場所から読み出され、ネットワーク４を介してクライアント側へ転送される（Ｓ１０２）。

【００７７】

復号化部２０では、公開鍵暗号方式を用いて、公開鍵ＩＤに対応した秘密鍵を用いて共通鍵がＳｋｅｙ２として復号される（Ｓ１０３）。

そして、この共通鍵Ｓｋｅｙ２を用いて、共通鍵暗号方式に基づきデータが「こんにちは」として復号される（Ｓ１０４）。

【００７８】

次に、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合、および特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合のＷＷＷサーバ３における動作を説明する。

【００７９】

まず、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合について説明する。

この場合、WWWサーバ３においては、グループリスト管理部３１１により、権限が確認されるとともに、グループＩＤを参照して特定グループ（たとえば、Ｂチーム）に属するメンバーの公開鍵番号（Ｎｏ）、公開鍵がグループリストＧＬから取得される。

そして、共通鍵管理部３１２で、グループの共通鍵リストＧＣＫＬよりグループＩＤが参照され、特定グループ（たとえば、Ｂチーム）で利用されている共通鍵番号（たとえば、５２、１１１、１２３）が全て検索される。

さらに、共通鍵管理部３１２において、共通鍵リストＣＫＬより、各共通鍵番号（たとえば、５２、１１１、１２３）とグループ管理者の公開鍵番号（たとえば、１１：ＡＡ）が一致する全ての暗号化鍵（たとえば、qwer、peha、gobp）が取得され、グループ管理者のクライアントに転送される。

【００８０】

グループ管理者の暗号化復号化装置１０では、グループリストと全ての暗号化鍵を復号化した共通鍵（たとえば、Ｓｋｅｙ１００、Ｓｋｅｙ１０５、Ｓｋｅｙ８０）が得られる。図６を参照して説明したように、グループリストの変更が行われた後、それらの共通鍵が、新規登録されたメンバーの公開鍵を利用して暗号化される（たとえば、xhen、mxco、henc）。

そして、これらの暗号化鍵とグループリスト、公開鍵番号（たとえば、Ｌ２：ＣＡ）と共通鍵ＩＤ（たとえば、５２、１１１、１２３）がWWWサーバ３に送信される。

【００８１】

グループリスト管理部３１１および共通鍵管理部３１２では、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とグループリスト、公開鍵番号（Ｎｏ）と共通鍵ＩＤを受けて、グループリストＧＬ、共通鍵リストＣＫＬ、グループの共通鍵リストＧＣＫＬが変更される。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含ま

れているので、過去の共有情報を取得することができるようになる。

【００８２】

次に、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合について説明する。

【００８３】

この場合、ＷＷＷサーバ３のグループリスト管理部３１１では、グループリストの更新が行われる。このとき、最後の返信部分では、新しいグループリストと更新前のグループリストとが比較され、削除したメンバーの公開鍵番号（Ｎｏ）が割り出される。そして、グループＩＤと削除したメンバーの公開鍵番号（Ｎｏ）が共通鍵管理部３１２にわたされる。

共通鍵管理部３１２では、グループの共通鍵リストＧＣＫＬより、グループＩＤを参照して、特定グループ（たとえば、Ｂチーム）で利用されていた共通鍵番号（たとえば、３８、４４４、１３３）が全て検索される。

次いで、共通鍵管理部３１２では、共通鍵リストＣＫＬより、各共通鍵番号（（たとえば、３８、４４４、１３３）と削除したメンバーの公開鍵番号（たとえば、ＬＬ：ＢＢ）が一致する全ての暗号化鍵が削除される。

【００８４】

なお、ＷＷＷサーバ３、具体的には、ＤＢＭＳ３１では、メンバーの追加と削除が同時に行われた場合には、上述した手法が組み合わされて実行される。

【００８５】

以上説明したように、本実施形態によれば、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されるＷＷＷサーバ３と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部１３と、情報を暗号化するための共通鍵を用いて上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部１１と、暗号化に用いた共通鍵を、記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部１４と、複数の暗号化鍵および暗号化データをＷＷ

Wサーバ３に転送し保管させる転送部１６と、WWWサーバ３からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみメンバーの公開鍵の追加または脱会するメンバーの公開鍵の削除を上記記憶部に対して行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送し保管させるリスト管理手段１７，１８，１９と、WWWサーバ３から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化部２０とを有する暗号化復号化装置１０とをインターネット４で接続したので、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

したがって、権限のない、サーバ等の情報保管装置の管理者の覗き見、改竄を防ぐことができる。

【００８６】

また、本実施形態では、情報保管装置としてのWWWサーバ３に、クライアント側からのグループリスト変更要求時に、グループリストＧＬにアクセスして、メンバー変更要求に対して応答し、返信されてきたグループ管理者の要求に従ってグループリストＧＬを変更可能なグループリスト管理部３１１と、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵を選択して、クライアントに転送する共通鍵管理部３１２と、グループの共通鍵リストＧＣＫＬ、共通鍵リストＣＫＬ、データ共通鍵リストＤＣＫＬ、暗号化データリストＥＤＬをアクセスし、クライアントの要求に従ってグループリストの送信と暗号化データの受付を行い、データＩＤを生成し、復号化要求を受け取った場合には、データＩＤと公開鍵番号（Ｎｏ）を参照し、３つのリストを参照して暗号化データと暗号化鍵を返信する暗号化データ保管部３１３とを設けたので、暗号化データを保管するデータベースや、サーバ、ファイルシステム等の情報保管装置を利用して共有されるユーザのデータが覗き見されたり、改竄されるおそれもなく、データの管理を確実に行うことができる。

【００８７】

なお、暗号化複合化装置１０におけるグループリストの作成、登録、削除、共通鍵の作成、登録、登録された共通鍵を用いたデータの暗号化、サーバ３に登録されたデータの復号処理工程を実行するためのプログラム、あるいはサーバ３におけるリストの変更、登録、保管等のプログラムは、第１および第２の端末装置（コンピュータ）１，２で読み出し可能な記録媒体、たとえば暗号化装置１０やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、端末装置で読み出されて実行される。

また、他の例としては、たとえばインターネットの専用線や電話回線等の通信線路のように、通信プログラムに伝送する際にこの通信プログラムを一定時間保持するデータ伝送路等を挙げることができる。

【００８８】

【発明の効果】

以上説明したように、本発明によれば、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムのグループ管理者に情報の内容を見られてしまう可能性もない。

【図面の簡単な説明】

【図１】

本発明に係る情報共有システムの基本的な構成図である。

【図２】

本発明に係る暗号化復号化装置の構成例を示すブロック図である。

【図３】

図２の復号化部の構成例を示す図である。

【図４】

ＷＷＷサーバの保管される各種リストを示す図である。

【図５】

本発明に係る情報管理装置としてのＷＷＷサーバにおけるＤＢＭＳの詳細な機能を説明するための図である。

【図６】

グループで共通鍵を共有する場合であって、グループへの公開鍵ＩＤの登録動作例を説明するための図である。

【図７】

グループで共通鍵を共有する場合であって、共通鍵の登録動作例を説明するための図である。

【図８】

グループで共通鍵を共有する場合であって、データを暗号化する場合の動作例を説明するための図である。

【図９】

共有したいユーザを別途してする場合であって、データを暗号化する場合動作例を説明するための図である。

【図１０】

復号化動作例を説明するための図である。

【符号の説明】

１…第１の端末装置

２…第２の端末装置

３…ＷＷＷサーバ（情報保管装置）

４…ネットワーク

１０…暗号化復号化装置

１１…暗号化部

１２…共通鍵生成部

１３…記憶部

１４…暗号化鍵生成部

１５…付加情報生成部

１６…転送部

１７…署名確認部

１８…公開鍵管理部

１９…署名付加部

２０…復号化部

３１…データベースマネージメントシステム（ＤＢＭＳ）

３１１…グループリスト管理部

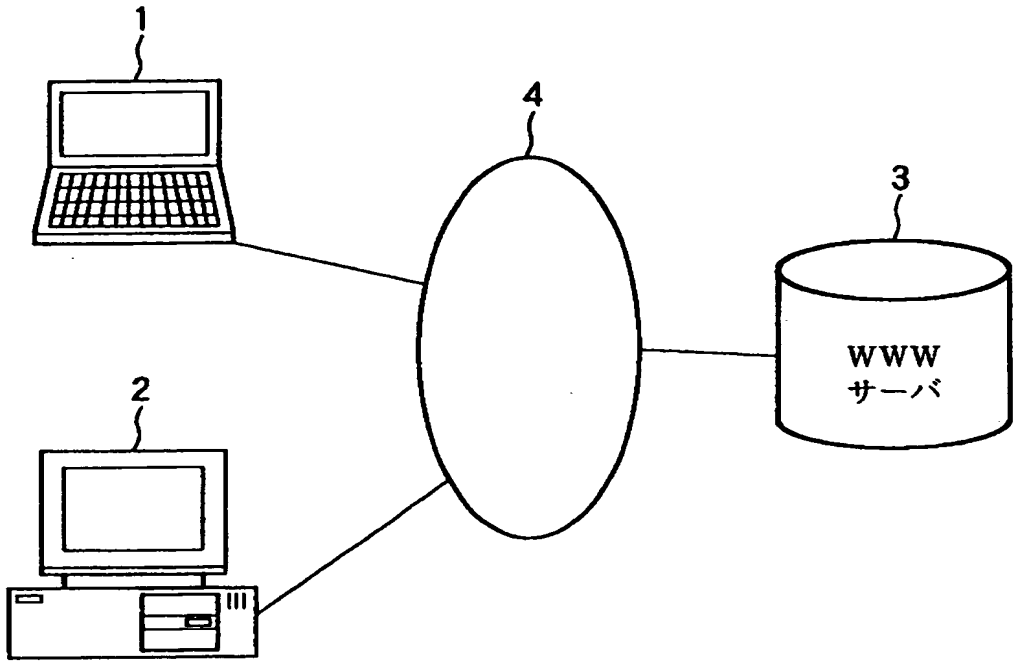
３１２…共通鍵管理部

３１３…暗号化データ管理部

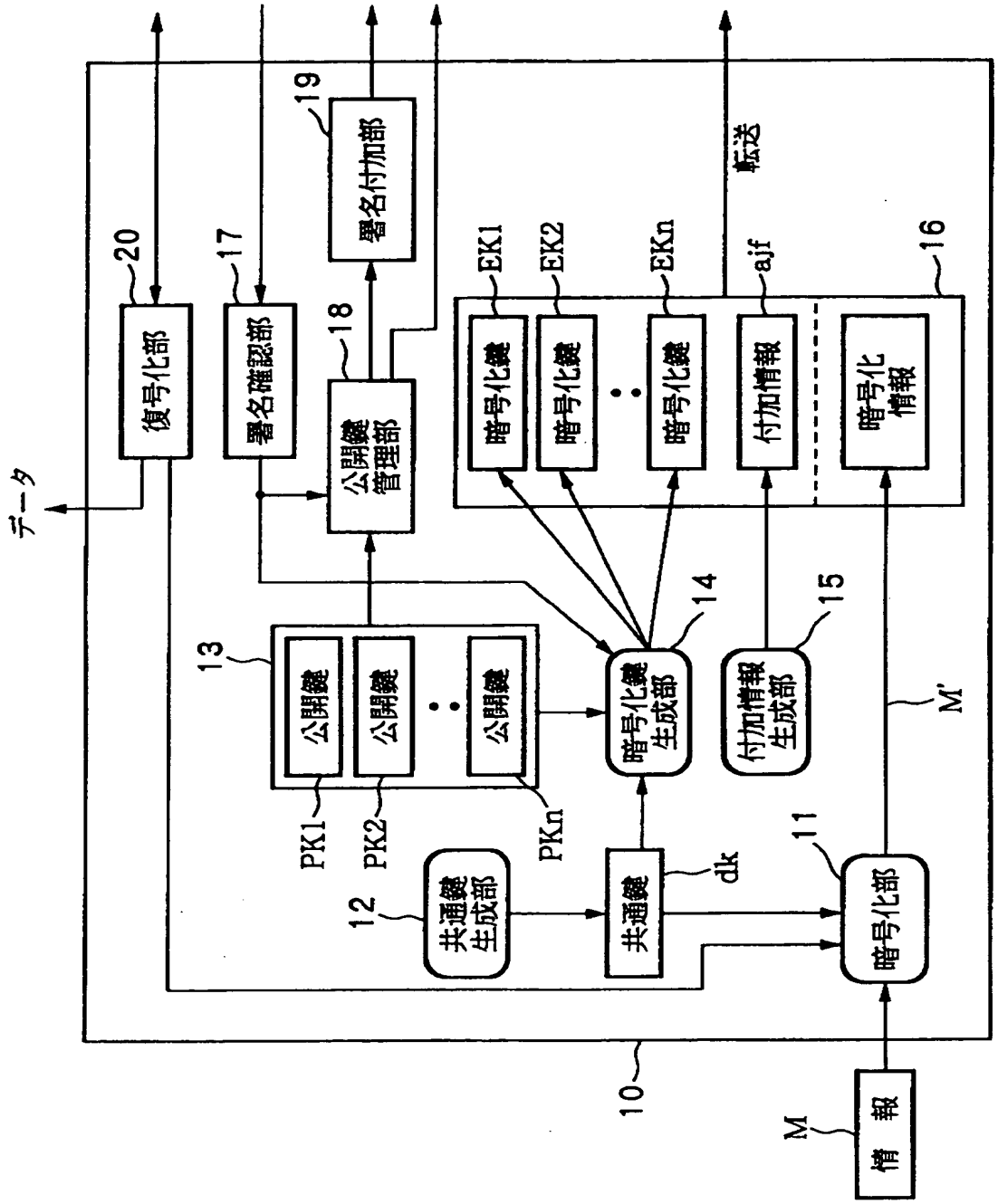
３２…権限確認部

【書類名】　図面

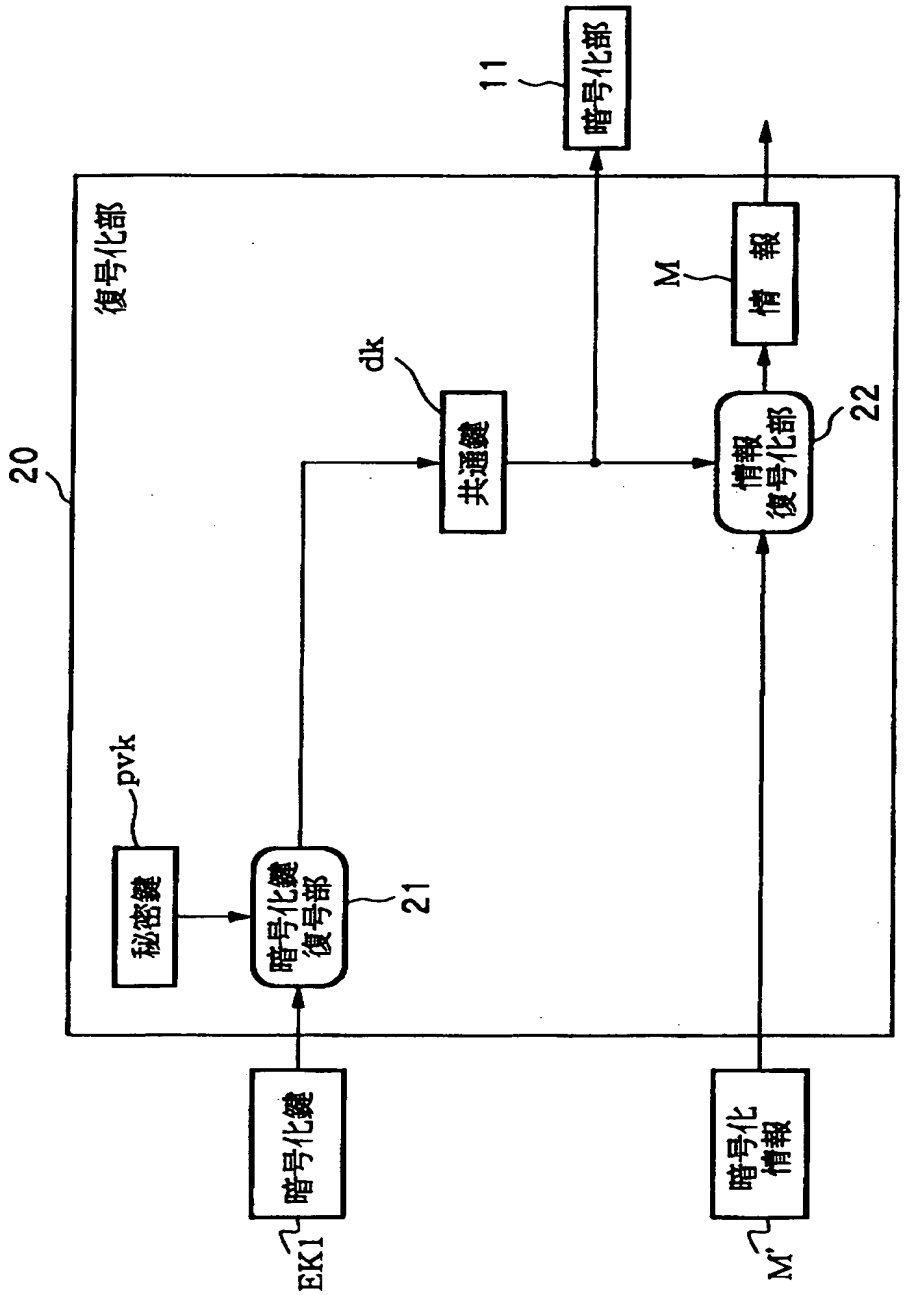
【図１】



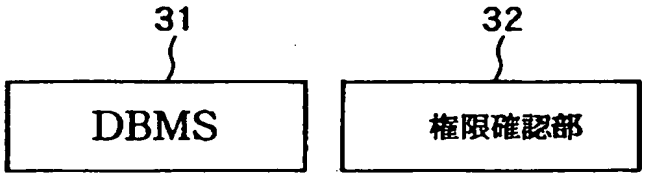
【図２】


データ
復号化部
20
署名確認部
17
署名付加部
19
公開鍵管理部
18
転送
EK1
EK2
EKn
ajf
16
暗号化鍵
暗号化鍵
暗号化鍵
付加情報
暗号化情報
13
公開鍵
公開鍵
公開鍵
14
暗号化鍵生成部
15
付加情報生成部
M'
PK1
PK2
PKn
12
共通鍵生成部
共通鍵
dk
11
暗号化部
10
M
情報

【図３】


暗号化部
11
復号化部
20
M
情報
dk
共通鍵
情報復号化部
22
pvk
秘密鍵
暗号化鍵復号部
21
暗号化鍵
EK1
暗号化情報
M'

【図４】



グループリストGL

グループID	公開鍵No	メンバー公開鍵	グループ管理者D署名
:	:	:	

共通鍵リストCKL

共通鍵No	公開鍵No	暗号化鍵
122	11:AA	qwer
122	1C:FF	zxcv
122	E5:4B	wert

グループの共通鍵リストGCKL

グループID	共通鍵No
Bチーム	123

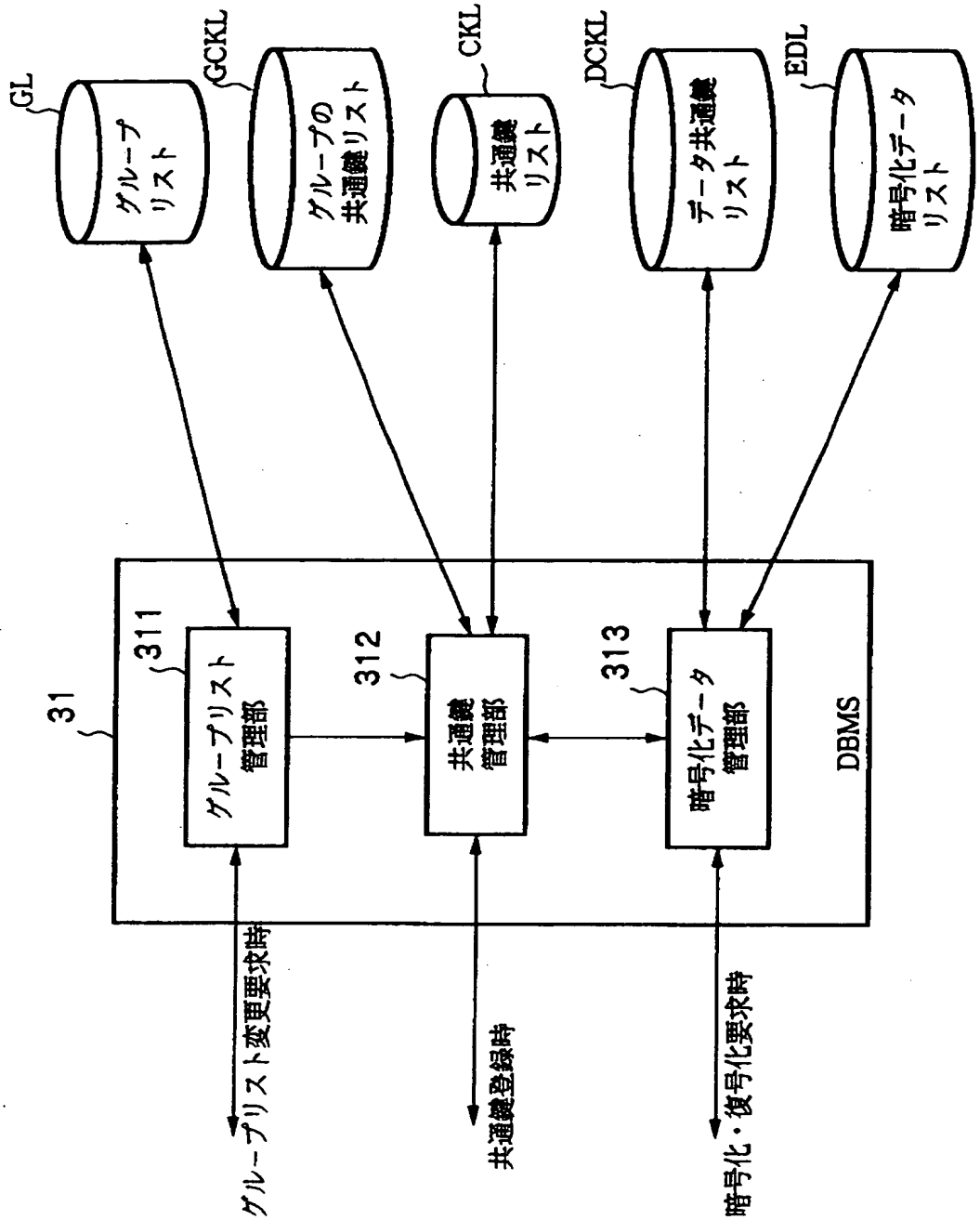
暗号化データリストEDL

データID	暗号化データ
4444	jjjjjjjjjjjj

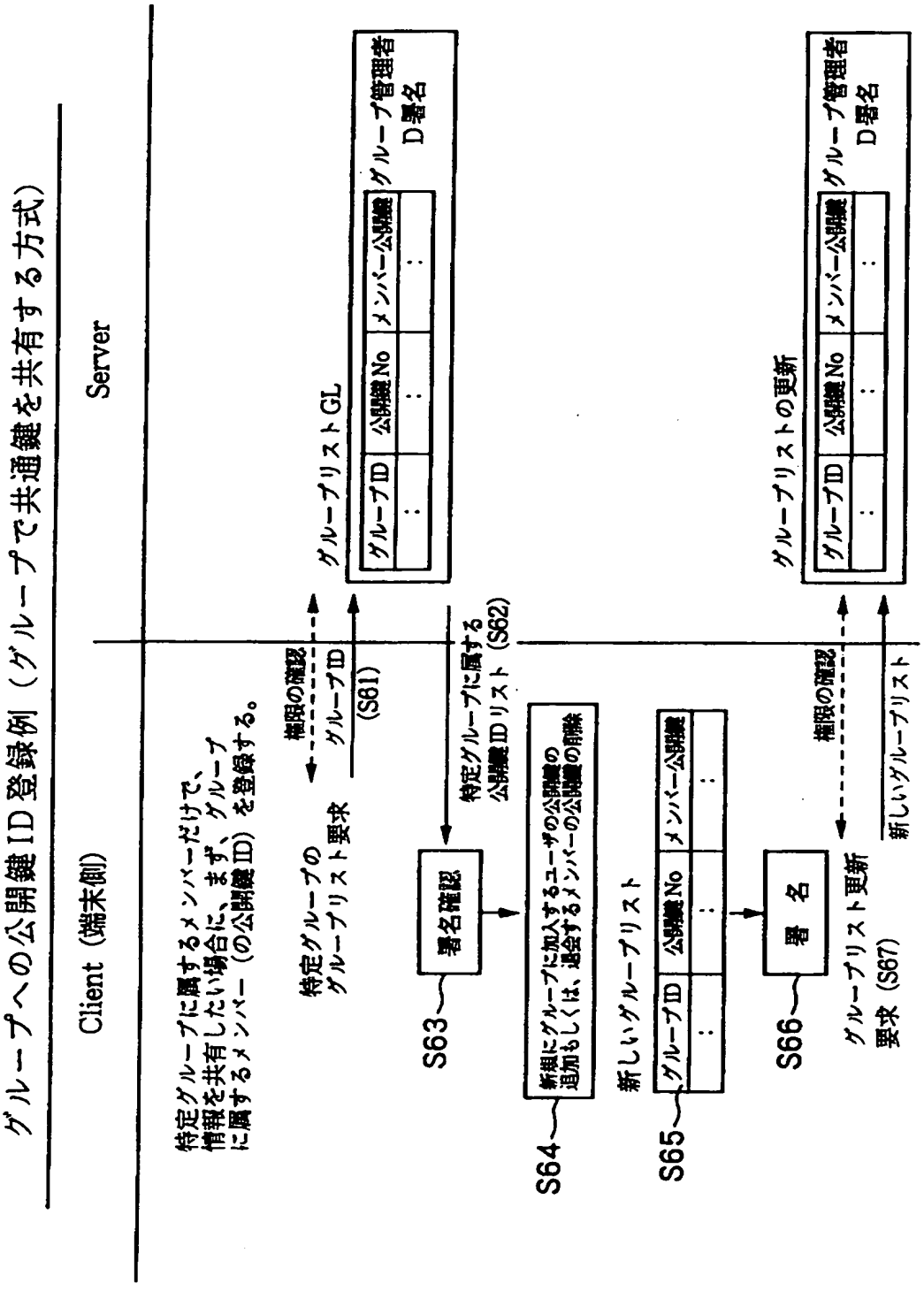
データ共通鍵リストDCKL

データID	共通鍵No
4444	123

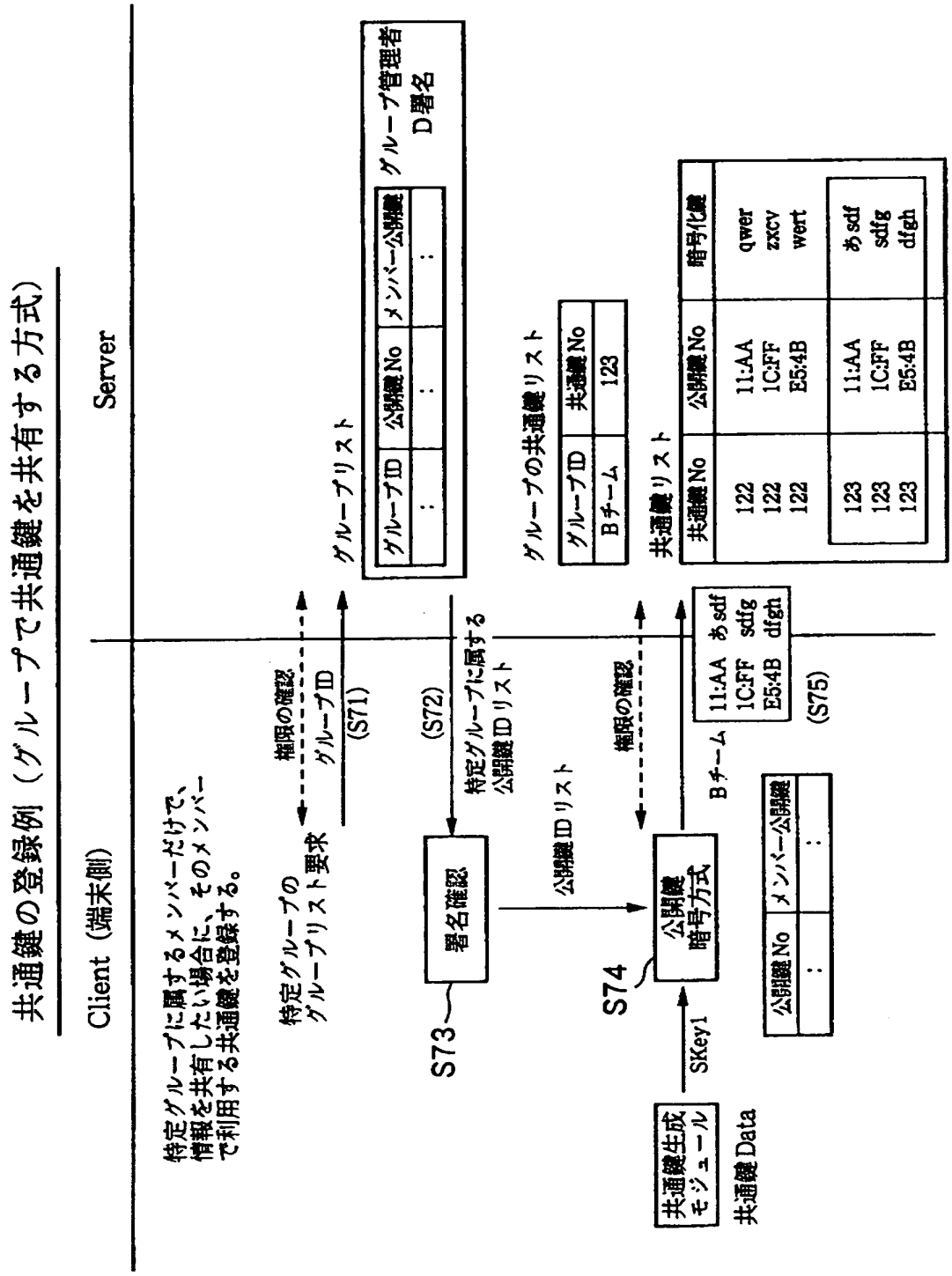
【図５】


GL
グループリスト
GCKL
グループの共通鍵リスト
CKL
共通鍵リスト
DCKL
データ共通鍵リスト
EDL
暗号化データリスト
31
311
グループリスト管理部
312
共通鍵管理部
313
暗号化データ管理部
DBMS
グループリスト変更要求時
共通鍵登録時
暗号化・復号化要求時

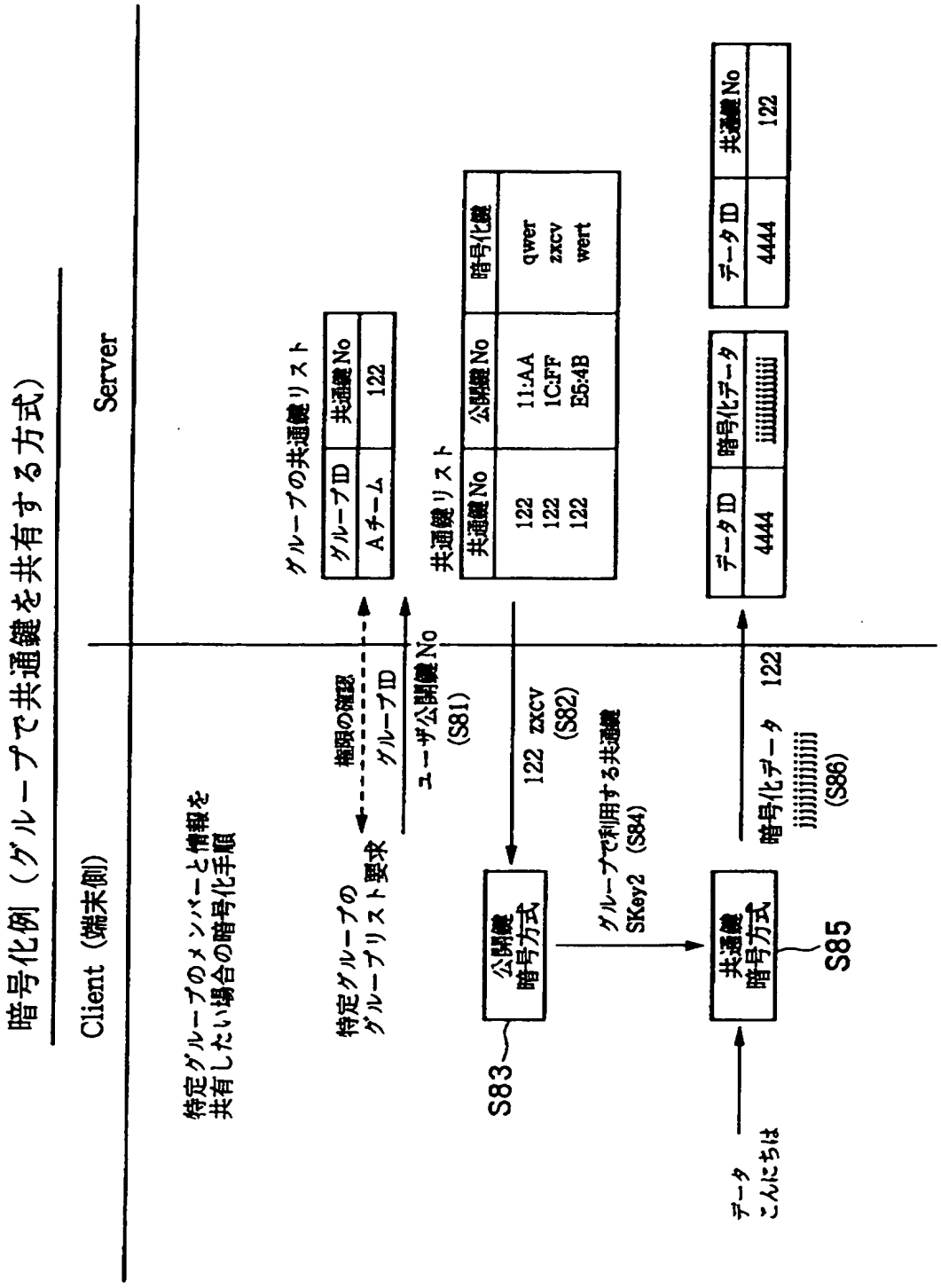
【図６】


グループへの公開鍵ID登録例（グループで共通鍵を共有する方式）
Client（端末側）
Server
特定グループに属するメンバーだけで、情報を共有したい場合に、まず、グループに属するメンバー（の公開鍵ID）を登録する。
権限の確認
グループID
(S61)
特定グループの
グループリスト要求
グループリストGL
グループID
公開鍵No
メンバー公開鍵
グループ管理者D署名
特定グループに属する
公開鍵IDリスト（S62）
S63
署名確認
S64
新規にグループに加入するユーザの公開鍵の追加もしくは、退会するメンバーの公開鍵の削除
新しいグループリスト
S65
S66
署名
グループリスト更新
要求（S67）
権限の確認
新しいグループリスト
グループリストの更新

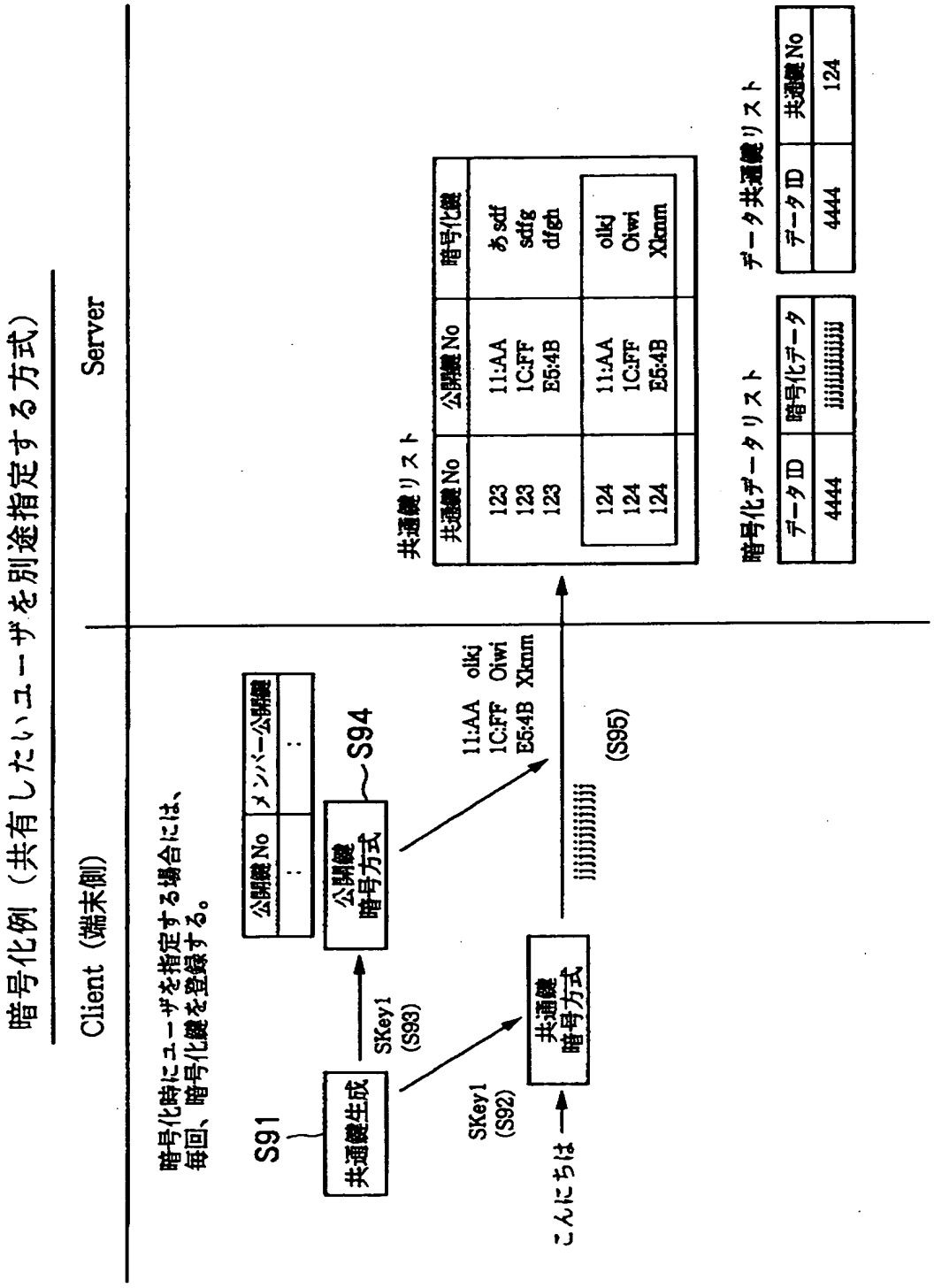
【図７】


共通鍵の登録例（グループで共通鍵を共有する方式）
Client（端末側）
Server
特定グループに属するメンバーだけで、情報を共有したい場合に、そのメンバーで利用する共通鍵を登録する。
特定グループのグループリスト要求
権限の確認
グループID
(S71)
グループリスト
グループID
公開鍵No
メンバー公開鍵
グループ管理者D署名
(S72)
特定グループに属する公開鍵IDリスト
S73
署名確認
公開鍵IDリスト
権限の確認
S74
公開鍵暗号方式
Bチーム
11:AA あsdf
1C:FF sdfg
E5:4B dfgh
(S75)
グループの共通鍵リスト
グループID
共通鍵No
Bチーム
123
共通鍵リスト
共通鍵No
公開鍵No
暗号化鍵
122 11:AA qwer
122 1C:FF zxcv
122 E5:4B wert
123 11:AA あsdf
123 1C:FF sdfg
123 E5:4B dfgh
公開鍵No
メンバー公開鍵
SKey1
共通鍵生成モジュール
共通鍵Data

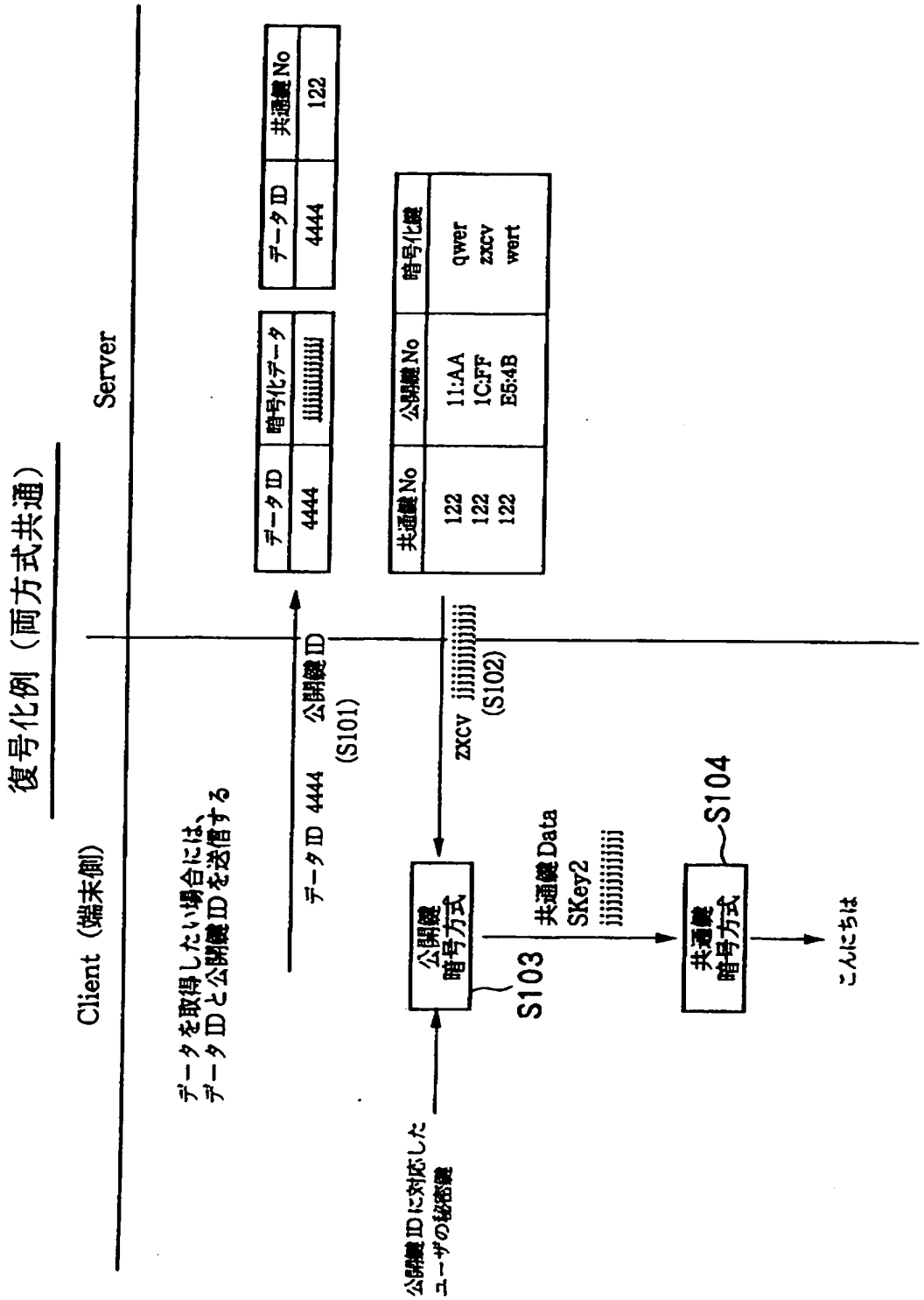
【図８】


暗号化例（グループで共通鍵を共有する方式）
Client（端末側）
Server
特定グループのメンバーと情報を
共有したい場合の暗号化手順
特定グループの
グループリスト要求
権限の確認
グループID
ユーザ公開鍵No
(S81)
グループの共通鍵リスト
グループID
共通鍵No
Aチーム
122
共通鍵リスト
共通鍵No
公開鍵No
暗号化鍵
122
122
122
11:AA
1C:FF
E5:4B
qwer
zxcv
wert
122 zxcv
(S82)
公開鍵
暗号方式
S83
グループで利用する共通鍵
SKey2 (S84)
共通鍵
暗号方式
S85
データID
暗号化データ
4444
jjjjjjjjjjjjjj
データID
共通鍵No
4444
122
暗号化データ 122
jjjjjjjjjjjjjj
(S86)
データ
こんにちは

【図９】


暗号化例（共有したいユーザを別途指定する方式）
Client（端末側）
Server
暗号化時にユーザを指定する場合には、
毎回、暗号化鍵を登録する。
S91
共通鍵生成
SKey1
(S93)
公開鍵No
メンバー公開鍵
公開鍵
暗号方式
S94
11:AA olkj
1C:FF Otwi
E5:4B Xkmm
(S95)
jjjjjjjjjjjjjj
SKey1
(S92)
共通鍵
暗号方式
こんにちは
共通鍵リスト
共通鍵No
公開鍵No
暗号化鍵
123 11:AA あsdf
123 1C:FF sdfg
123 E5:4B dfgh
124 11:AA olkj
124 1C:FF Otwi
124 E5:4B Xkmm
暗号化データリスト
データID
暗号化データ
4444 jjjjjjjjjjjjjj
データ共通鍵リスト
データID
共通鍵No
4444 124

【図１０】


復号化例（両方式共通）
Client（端末側）
Server
データを取得したい場合には、
データIDと公開鍵IDを送信する
データID 4444
公開鍵ID
(S101)
データID
暗号化データ
4444
jjjjjjjjjjjjjj
共通鍵No
122
データID
4444
zxcv jjjjjjjjjjjjjj
(S102)
公開鍵No
暗号化鍵
122
122
122
11:AA
1C:FF
E5:4B
qwer
zxcv
wert
公開鍵
暗号方式
S103
共通鍵Data
SKey2
jjjjjjjjjjjjjj
共通鍵
暗号方式
S104
こんにちは
公開鍵IDに対応した
ユーザの秘密鍵

【書類名】　　要約書

【要約】

【課題】暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改竄を防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供する。

【解決手段】ＷＷＷサーバ３からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみメンバーの公開鍵の追加または脱会するメンバーの公開鍵の削除を記憶部１３に対して行い、追加登録または削除を行う場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成してＷＷＷサーバ３に転送するリスト管理手段１７，１８，１９を設ける。

【選択図】　　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000006264
【住所又は居所】　東京都千代田区大手町１丁目５番１号
【氏名又は名称】　三菱マテリアル株式会社
【代理人】　申請人
【識別番号】　100094053
【住所又は居所】　東京都台東区柳橋２丁目４番２号　創進国際特許事務所
【氏名又は名称】　佐藤　隆久

出　願　人　履　歴　情　報

識別番号　　〔０００００６２６４〕

１．変更年月日　　１９９２年　４月１０日
　［変更理由］　　住所変更
　　住　所　　東京都千代田区大手町１丁目５番１号
　　氏　名　　三菱マテリアル株式会社